PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-337924
(43)Date of publication of application : 07.12.2001

(51)Int.Cl. G06F 15/00

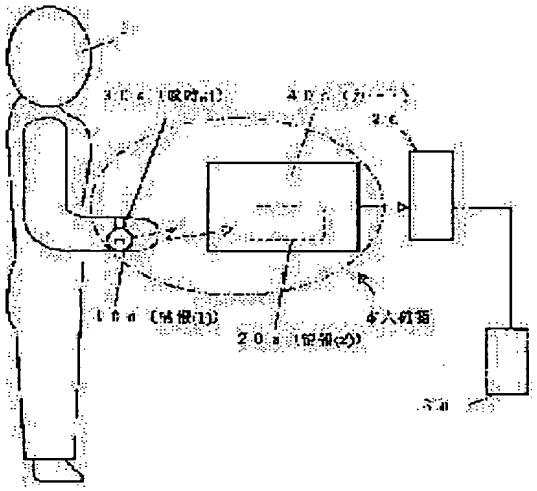
(21)Application number : 2001-071217
(22)Date of filing : 13.03.2001

(71)Applicant : TIETECH CO LTD
HASHIMOTO HIDENORI
(72)Inventor : HASHIMOTO HIDENORI
FUKATSU HIROICHI

(30)Priority
Priority number : 2000128648 Priority date : 23.03.2000 Priority country : JP

(54) PERSON CONFIRMING METHOD AND PERSON CONFIRMING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a person confirming method and a person confirming device having high reliability at a low cost.
SOLUTION: A user uses a user portable device 10a provided on a user portable apparatus 30a in which the user can carry and a user device 20a provided on a user apparatus (a card or a cellular phone) 40a used by the user. One information (original information) as a whole is divided to obtain first information and second information. The user portable device 10a holds the first information, and the user device 20a holds the second information. The user device 20a combines the received information and the second information held by the user himself. When the user can generate the original information by combining the received information and the second information, the user 1 is confirmed as the primary user of the user apparatus 40a and allowed to use the user apparatus 40a.



LEGAL STATUS
[Date of request for examination] 15.03.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－337924
（P2001－337924A）
(43)公開日　平成13年12月７日(2001.12.7)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ　５Ｂ０８５

審査請求　未請求　請求項の数13　ＯＬ　（全 13 頁）

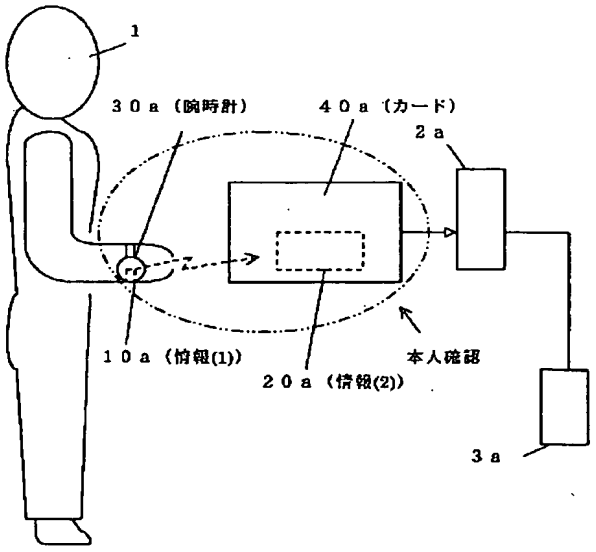
(21)出願番号　特願2001－71217(P2001－71217)
(22)出願日　平成13年３月13日(2001.3.13)
(31)優先権主張番号　特願2000－128648(P2000－128648)
(32)優先日　平成12年３月23日(2000.3.23)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　391006348
株式会社タイテック
愛知県名古屋市南区千竈通２丁目13番地１
(71)出願人　500200627
橋本　秀紀
東京都港区赤坂九丁目５番27号　ルピナス赤坂乃木坂302号
(72)発明者　橋本　秀紀
東京都港区赤坂九丁目５番27号　ルピナス赤坂乃木坂302号
(74)代理人　100064344
弁理士　岡田　英彦　（外３名）

最終頁に続く

(54)【発明の名称】　本人確認方法及び本人確認装置

(57)【要約】
【課題】　低コストで、信頼性の高い本人確認方法及び本人確認装置を提供する。
【解決手段】　ユーザが携帯可能なユーザ携帯機器３０ａに設けられるユーザ携帯装置１０ａと、ユーザが使用するユーザ機器（カードや携帯電話機）４０ａに設けられるユーザ装置２０ａを用いる。全体として一つの情報（原情報）を分割し、第１情報と第２情報を得る。ユーザ携帯装置１０ａに第１情報を保有させ、ユーザ装置２０ａに第２情報を保有させる。ユーザ装置２０ａは、受信した情報と自身が保有する第２情報を結合する。そして、受信した情報と第２情報を結合して原情報を作成することができた場合には、ユーザ１がユーザ機器４０ａの本来のユーザであることを確認し、ユーザ機器４０ａの使用を可能とする。



【特許請求の範囲】
【請求項１】　ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認方法であって、
原情報を第１情報と第２情報に分割し、第１情報をユーザが携帯するユーザ携帯装置に保有させるとともに、第２情報をユーザが使用するユーザ機器に設けられるユーザ装置に保有させるステップと、
ユーザ携帯装置から第１情報を送信するステップと、
ユーザ装置で情報を受信するステップと、
ユーザ装置で受信した情報とユーザ装置が保有している第２情報とを結合し、原情報を作成することができた場合に本人であることを確認するステップと、を備える本人確認方法。
【請求項２】　請求項１に記載の本人確認方法であって、
ユーザ携帯装置から第１情報を送信するステップでは、第１情報を暗号化して送信し、
ユーザ装置で情報を受信するステップでは、受信した情報を解読する、本人確認方法。
【請求項３】　請求項１に記載の本人確認方法であって、
ユーザ携帯装置から第１情報を送信するステップでは、第１情報にランダムノイズを挿入し、
ユーザ装置で情報を受信するステップでは、受信した情報からランダムノイズを除去する、本人確認方法。
【請求項４】　請求項１～３のいずれかに記載の本人確認方法であって、ユーザ携帯装置から第１情報を送信するステップでは、第１情報を無線で送信する、本人確認方法。
【請求項５】　請求項１～３のいずれかに記載の本人確認方法であって、
更に、ユーザ装置から情報送信要求信号を送信するステップを備え、
ユーザ携帯装置から第１情報を送信するステップでは、ユーザ携帯装置が情報送信要求信号を受信した時に第１情報を送信する、本人確認方法。
【請求項６】　ユーザ機器を使用する人がそのユーザ機器の本来のユーザであることを確認する本人確認装置であって、
ユーザが携帯するユーザ携帯装置と、
ユーザが使用するユーザ機器に設けられるユーザ装置とを備え、
ユーザ携帯装置は、原情報を分割して得た第１情報と第２情報のうちの第１情報を記憶する第１記憶手段と、第１記憶手段に記憶されている第１情報を送信する第１通信手段とを有し、
ユーザ装置は、原情報を分割して得た第１情報と第２情報のうちの第２情報を記憶する第２記憶手段と、第２通信手段と、第２通信手段で受信した情報と第２記憶手段に記憶している第２情報を結合し、原情報を形成することができた場合に本人であることを確認する本人確認手段とを有する、本人確認装置。
【請求項７】　請求項６に記載の本人確認装置であって、ユーザ携帯装置は、所定時間毎に第１情報を送信する、本人確認装置。
【請求項８】　請求項６に記載の本人確認装置であって、
ユーザ装置は、情報送信要求信号を送信し、
ユーザ携帯装置は、情報送信要求信号を受信した時に第１情報を送信する、本人確認装置。
【請求項９】　請求項６～８のいずれかに記載の本人確認装置であって、ユーザ機器には、第２情報の不正な読み出しを検出した時に、第２情報の読み出しを禁止する読出禁止手段が設けられている、本人確認装置。
【請求項１０】　請求項９に記載の本人確認装置であって、読出禁止手段は、第２記憶手段を破壊する、本人確認装置。
【請求項１１】　請求項６～１０のいずれかに記載の本人確認装置であって、ユーザ携帯装置及びユーザ装置の少なくとも一方の、少なくとも一部はＩＣチップにより構成されている、本人確認装置。
【請求項１２】　請求項１１に記載の本人確認装置であって、ＩＣチップあるいはＩＣチップの記憶手段に記憶されている情報を交換可能に構成されている、本人確認装置。
【請求項１３】　請求項６～１２のいずれかに記載の本人確認装置であって、本人確認手段は、本人であることを確認した場合にユーザ機器の使用を許可する本人確認装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ユーザ機器を使用するユーザがそのユーザ機器の本来のユーザであることを（本人であること）を確認する本人確認方法及び本人確認装置に関する。特に、認証が必要であるシステムに好適に用いることができる本人確認方法及び本人確認装置に関する。
【０００２】
【従来の技術】ユーザがサービス会社のサービスを利用する場合、サービス会社は、サービスを利用しようとするユーザが本人であることを確認するために、認証を行っている。認証方法としては、例えば、暗証番号を用いる方法、サイン用いる方法、印章を用いる方法、ＩＤコード（非接触でユーザ機器へＩＤコードを送信または送受信する小型通信機）を用いる方法等が使用されている。暗証番号を用いる方法は、例えば、キャッシュカードを用いて銀行の口座から現金を引き出す場合に用いられる。ユーザは、現金を引き出す場合、銀行のＡＴＭ（現金自動支払機）のカード挿入口にキャッシュカード

を挿入し、暗証番号を入力する。ＡＴＭは、キャッシュカードから読み取ったカード情報（例えば、ＩＤ）とユーザが入力した暗証番号を認証センタに送信する。認証センタは、ＡＴＭに入力された暗証番号及び読み取ったカード情報と、記憶手段に記憶されているカード情報と暗証番号との対応関係を含むデータベースに基づいて、認証を行う。サインを用いる方法は、例えば、クレジットカードを用いて商品の代金を支払う場合に用いられる。ユーザは、クレジットカードで代金を支払う場合、商品購入票にサインをする。商品販売者は、商品購入票のサインとクレジットカードに記入されているサインを比較することによって認証を行う。印章を用いる方法は、例えば、預金通帳を用いて銀行の口座から現金を引き出す場合に用いられる。ユーザは、預金通帳を用いて銀行の口座から現金を引き出す場合、現金引出用紙に印鑑を用いて押印する。銀行は、現金引出用紙に押印された印章と予め登録されている印章とを比較することによって認証を行う。ＩＤコードを用いる方法は、例えば、ユーザが使用するユーザ機器の不正使用を防止する場合等に用いられる。この方法では、ユーザが携帯するタグ（送受信機能付きのカード部材等）及びユーザが使用するユーザ機器（例えば、携帯電話）に同じＩＤコードを記憶させる。タグは、ユーザ機器に接続して使用することもできるが、無線タグとして使用する場合が多い。ユーザ機器は、タグから送信されたＩＤコードと自己が記憶しているＩＤコードとを照合し、一致している場合にはユーザ機器の使用制限を解除（使用許可信号を出力）する。また、ユーザ本人であることを確認する他の認証方法として、各人に固有の生体情報（声紋、指紋、掌紋、網膜パターン、顔を撮像した画像等）を用いる方法が知られている。この認証方法では、生体情報読取装置によってユーザの生体情報を読み取り、読み取った生体情報と予め登録されている生体情報とを照合することによって認証を行うものである。この認証方法は、各人に固有の生体情報を用いるため、認証精度が高い。

【０００３】

【発明が解決しようとする課題】暗証番号、サイン、印章やＩＤコードによって本人確認を行う従来の本人確認方法は、キャッシュカードを使用した人、クレジットカードを使用した人、預金通帳を使用した人、ＩＤコードを記憶させたタグを携帯する人が本来のユーザでない場合でも、正しいユーザであると認証してしまうことがある。例えば、ユーザ機器（例えば、キャッシュカード）や印鑑等の盗難、暗証番号、サインやＩＤコード等の情報盗難や情報漏洩が発生すると、ユーザ機器が不正使用されてしまう。また、生体情報によって本人確認を行う従来の本人確認方法は、生体情報読取装置（例えば、撮像手段）や生体情報処理装置（例えば、画像処理装置、大容量の記憶装置）等が必要であるため、システム全体のコストが高くなる。また、指に傷がついた場合や眼病になった場合には、指紋や網膜パターンが変化し、認証精度が低下する可能性がある。また、網膜パターンを用いる場合には、目を測定位置に持って行く必要があるため、煩わしさがある。また、指紋を用いる場合には、指を指紋読取装置に接触させる必要があるため、きれい好きの人にとっては心理的不快感がある。そこで、本発明は、低コストで信頼性の高い本人確認方法及び本人確認装置を提供することを目的とする。

【０００４】

【課題を解決するための手段】前記課題を解決するための本発明の第１発明は、請求項１に記載されたとおりの本人確認方法である。請求項１に記載の本人確認方法では、原情報を第１情報と第２情報に分割し、第１情報をユーザが携帯するユーザ携帯装置に保有させるとともに、第２情報をユーザが使用するユーザ機器に設けられるユーザ装置に保有させ、ユーザ装置は、受信した情報と自己が保有している情報とを結合して原情報を形成することができた場合に、本人であることを確認する。請求項１に記載の本人確認方法を用いれば、生体情報を用いる場合に比べて安価に構成することができる。また、暗証番号やカードを盗まれても不正使用の心配がない。また、ユーザ携帯装置とユーザ装置には原情報を分割した第１情報及び第２情報を記憶させている（同じ情報でない）ため、ユーザ使用機器が盗まれても不正使用の心配がない。これにより、暗証番号、サイン、印章、ＩＤコード等を用いる場合に比べて信頼性が高い。また、本発明の第２発明および第３発明は、請求項２および請求項３に記載されたとおりの本人確認方法である。請求項２および請求項３に記載の本人確認方法用いれば、ユーザ携帯装置とユーザ装置との間で暗号化された情報あるいはランダムノイズが挿入された情報を送受信するため、一層信頼性が向上する。また、本発明の第４発明は、請求項４に記載されたとおりの本人確認方法である。請求項４に記載の本人確認方法を用いれば、ユーザ携帯装置とユーザ装置との間で無線で情報を伝送するため、使い勝手が良く、また安価に構成することができる。また、本発明の第５発明は、請求項５に記載されたとおりの本人確認方法である。請求項５に記載の本人確認方法では、ユーザ装置は、本人確認を行う必要がある時に、ユーザ携帯装置に情報送信要求信号を送信し、ユーザ携帯装置から第１情報を受信する。これにより、ユーザ携帯装置の消費電力を低減することができる。また、本発明の第６発明は、請求項６に記載されたとおりの本人確認装置である。請求項６に記載の本人確認装置では、原情報を第１情報と第２情報に分割し、第１情報をユーザが携帯するユーザ携帯装置に保有させるとともに、第２情報をユーザが使用するユーザ機器に設けられるユーザ装置に保有させ、ユーザ装置は、受信した情報と自己が保有している情報とを結合して原情報を形成することができた場合に、本人であることを確認する。請

求項６に記載の本人確認装置を用いれば、生体情報を用いる場合に比べて安価に構成することができ、暗証番号やカードを盗まれても不正使用の心配がない。また、ユーザ携帯装置とユーザ装置には原情報を分割した第１情報及び第２情報を記憶させている（同じ情報でない）ため、ユーザ使用機器が盗まれても不正使用の心配がない。これにより、暗証番号、サイン、印章、ＩＤコード等を用いる場合に比べて信頼性が高い。また、本発明の第７発明は、請求項７に記載されたとおりの本人確認装置である。請求項７に記載の本人確認装置を用いれば、ユーザ携帯装置は、所定時間毎に第１情報を送信するため、ユーザ装置は、本人であるか否かを常時確認することができる。また、本発明の第８発明は、請求項８に記載されたとおりの本人確認装置である。請求項８に記載の本人確認装置では、ユーザ装置は、例えば、本人確認を行う必要がある時に、ユーザ携帯装置に情報送信要求信号を送信し、ユーザ携帯装置から第１情報を受信する。これにより、ユーザ携帯装置の消費電力を低減することができる。また、本発明の第９発明は、請求項９に記載されたとおりの本人確認装置である。請求項９に記載の本人確認装置では、ユーザ機器には、ユーザ装置に記憶されている第２情報の不正な読み出しを検出した時に第２情報の読み出しを禁止する読出禁止手段が設けられている。これにより、第２情報が不正に読み出されるのを防止することができ、信頼性が一層向上する。また、本発明の第１０発明は、請求項１０に記載されたとおりの本人確認装置である。請求項１０に記載の本人確認装置では、読出禁止手段は、第２記憶手段を破壊する。このため、簡単な構成で、ユーザ装置に記憶されている第２情報が不正に読み取られるのを防止することができる。また、本発明の第１１発明は、請求項１１に記載されたとおりの本人確認装置である。請求項１１に記載の本人確認装置では、ユーザ携帯装置及びユーザ装置の少なくとも一方の、少なくとも一部はＩＣチップにより構成されている。これにより、製造が容易であり、部品交換作業も容易となる。また、本発明の第１２発明は、請求項１２に記載されたとおりの本人確認装置である。請求項１２に記載の本人確認装置を用いれば、例えば、ユーザ携帯装置に記憶されている第１情報やユーザ装置に記憶されている第２情報が漏洩している可能性がある場合には、簡単に情報を変更することができるため、信頼性が向上する。また、本発明の第１３発明は、請求項１３に記載されたとおりの本人確認装置である。請求項１３に記載の本人確認装置を用いれば、本人確認手段が本人であることを確認した場合にのみ、ユーザ機器の使用が可能となるため、信頼性が向上する。

【０００５】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。本発明に対応する本人確認方法の第１の実施の形態の概略図を図１に示す。なお、図１は、本発明の本人確認方法を用いて認証システムを構成した図を示している。例えば、ユーザ１が、ユーザ機器の一種であるデビットカード４０ａを用いて決裁を行う場合（購入品の代金の支払い）、従来の認証方法では、以下のようにしてユーザ認証が行われる。まず、ユーザ１は、デビットカード４０ａを認証端末装置２ａのカード挿入口に挿入するとともに、暗証番号を入力手段等を用いて入力する。認証端末装置２ａは、デビットカード４０ａに記憶されているカード情報（ＩＤ等）を読み取り、読み取ったカード情報と、ユーザ１が入力した暗証番号を含むユーザ情報を認証センタ３ａに送信する。認証センタ３ａは、認証端末装置２ａから送信されたカード情報及び暗証番号と、暗証番号をカード情報に対応させて記憶しているデータベースとを照合することによって認証を行う。そして、認証センタ３ａは、認証がＯＫであれば、認証ＯＫ信号を認証端末装置２ａに送信し、認証がＮＧであれば、認証ＮＧ信号を認証端末装置２ａに送信する。

【０００６】この認証処理では、前述したように、ユーザ１がデビットカード４０ａの本来のユーザであることの確認（本人確認）は行われていない。そこで、本実施の形態では、認証センタ３ａでユーザ認証処理が行われる前に、本人確認処理（図１の二点鎖線で囲んだ部分）が以下のように行われる。本実施の形態では、本人確認装置は、ユーザ１が携帯するユーザ携帯機器（例えば、腕時計）３０ａに設けられたユーザ携帯装置１０ａと、ユーザが使用するユーザ機器（例えば、デビットカード）４０ａに設けられたユーザ装置２０ａにより構成される。ユーザ携帯装置１０ａとユーザ装置２０ａは、例えば、ユーザ認証を行うサービス会社が用意する。ユーザ携帯装置１０ａ、ユーザ装置２０ａを、ユーザ携帯機器３０ａ、ユーザ機器４０ａに取り付ける方法は種々の方法が可能である。例えば、接着剤や接着テープ等の取付手段を用いる方法、ユーザ携帯機器３０ａやユーザ機器４０ａに内蔵する方法等を用いることができる。また、本実施の形態では、ユーザ装置２０ａは、例えば、本人であることを確認できるまでは、使用禁止信号を出力してデビットカード４０ａを使用不能状態とする。すなわち、認証端末装置２ａがデビットカード４０ａのカード情報を読み出すことができないようにする。ユーザ携帯装置１０ａとユーザ装置２０ａには、本人確認に必要な情報が記憶されている。例えば、元々一つの情報として認識される情報（原情報）を分割し、一方の分割情報（情報(1)）をユーザ携帯機器３０ａに設けられたユーザ携帯装置（１０ａ）に保有（記憶）させ、他方の分割情報（情報(2)）をユーザ機器４０ａに設けられたユーザ装置２０ａに保有（記憶）させる。原情報を分割する方法としては、種々の方法を用いることができる。なお、ユーザ携帯機器３０ａは、腕時計に限定されず、ユーザ１が携帯可能あるいは携行可能であればよい。ま

た、ユーザ携帯装置１０ａは、ユーザ携帯機器３０ａと共に携帯する必要はなく、例えば、ポケットやカバンに入れて携帯してもよい。また、ユーザ機器４０ａは、カードに限定されず、本人確認が必要な機器であればよい。例えば、携帯電話やパソコン等でもよい。ユーザ機器４０ａは、複数のユーザが共用するものであってもよい。ユーザ携帯装置１０ａは、情報(1)をユーザ装置２０ａに送信する送信手段を備えている。情報(1)を送信する方法としては、無線電波を用いてもよいし、超音波や光（赤外線）を用いてもよい。

【０００７】ユーザ装置２０ａは、情報(1)を受信すると、受信した情報(1)と自身が記憶している情報(2)を所定のアルゴリズム（結合方法）で結合して情報(3)を作成（形成）する。そして、情報(3)と原情報を照合することによって本人確認を行う。すなわち、受信した情報(1)と自身が記憶している情報(2)を用いて原情報を再生あるいは復元することができた場合に、本人であることを確認する。前記したように、対応するユーザ携帯装置１０ａとユーザ装置２０ａには、同一の原情報から生成された分割情報（情報(1)と情報(2)）を記憶させている。このため、ユーザ装置２０ａは、正しい情報(1)を受信した場合にだけ、原情報を再生あるいは復元することができる。図１に示す認証システムでは、ユーザ機器であるデビットカード４０ａは、ユーザ１が本人であることを確認した場合にのみ、自身が記憶しているカード情報を認証端末装置２ａで読み取り可能とする。以上のように、デビットカード４０ａは、本人確認処理を行った後に、自身が記憶しているカード情報を認証端末装置２ａに出力するように構成されている。ここで、デビットカード４０ａを紛失し、盗まれ、あるいは、暗証番号を他人に知られた場合には、デビットカード４０ａは、そのデビットカード４０ａの本来のユーザが携帯しているユーザ携帯装置１０ａから送信される情報(1)を受信することができない。このため、認証センタ３ａでユーザ認証が行われる前に、デビットカード４０ａに設けられているユーザ装置２０ａの本人確認処理によって不正使用を確実に阻止することができる。

【０００８】本実施の形態では、割り符のように、一つの原情報を情報(1)（第１情報）と情報(2)（第２情報）に分割し、一方の情報(1)をユーザ携帯装置１０ａに記憶させ、他方の情報(2)をユーザ装置２０ａに記憶させている。そして、ユーザ装置２０ａは、正しい情報(1)を受信した場合に本人であることを確認する。したがって、生体情報を用いる場合に比して、安価に構成することができる。また、暗証番号やカードを盗まれたり、紛失したりしても、ユーザ携帯機器（ユーザ携帯装置）を盗まれたり、紛失したりしない限り、不正使用の心配がない。また、ユーザ携帯装置１０ａとユーザ装置２０ａには異なる情報を記憶させているので、一方が盗まれたり、紛失しても不正使用の心配がない。したがって、暗証番号、サイン、ＩＤデータ等を用いる場合に比べて、確実に本人確認を行うことができる。なお、本発明は、ユーザがユーザ機器を使用する際に、ユーザがそのユーザ機器の本当のユーザであるか否かを確認（本人確認）するための方法に関するものである。したがって、ユーザ機器で本人確認処理を行った結果をどのように利用するかは、ユーザ機器の種類やユーザ機器を利用する形態に応じて適宜選択される事項である。例えば、図１では、ユーザ装置２０ａは、本人であることを確認すると、デビットカード（ユーザ機器）４０ａのカード情報の認証端末装置２ａへの出力を許可する。これにより、デビットカード４０ａのカード情報が認証端末装置２ａで読み取られる。また、ユーザ１は、認証端末装置２ａの入力手段等を用いて暗証番号を入力する。以後は、従来例と同様の手順で、各認証センタ３ａでユーザ認証処理（デビットカードの正当性を認証する処理）を行う。

【０００９】次に、本実施の形態の本人確認装置を用いて本人確認処理を行う場合の手順を説明する。図２は、本人確認方法の処理手順の１例を説明する図である。本実施例では、ユーザ装置２０は、常時本人確認処理を行う。本実施例では、①～④の手順で本人確認処理が行われる。

①ユーザ携帯装置１０は、適宜の時期に（例えば、所定の時間間隔で）、自身が保有（記憶）している情報(1)を送信する。

②受信待機状態にあるユーザ装置２０は、情報(1)を受信する。

③ユーザ装置２０は、情報(1)を受信すると、受信した情報(1)と自身が記憶している情報(2)を所定のアルゴリズムで結合して情報(3)を形成する。

④ユーザ装置２０は、情報(3)と原情報を照合して、情報(3)と原情報が一致した場合（情報(1)と情報(2)を結合して原情報を形成することができた場合）には、ユーザが本人であることを確認する。

【００１０】図３は、本発明の本人確認方法の処理手順の他の例を説明する図である。本実施例では、ユーザ装置は、本人確認が必要な場合に本人確認処理を行う。本実施例では、①～⑥の手順で本人確認処理が行われる。

①ユーザ装置２０は、本人確認処理を行う必要がある場合（例えば、デビットカードが認証端末装置のカード挿入口に挿入された場合等）に、情報(1)の送信要求信号を送信する。

②受信待機状態にあるユーザ携帯装置１０は、情報(1)の送信要求信号を受信する。

③ユーザ携帯装置１０は、情報(1)の送信要求信号を受信すると、自身が記憶している情報(1)を送信する。

④受信待機状態にあるユーザ装置２０は、情報(1)を受信する。

⑤ユーザ装置２０は、情報を受信すると、受信した情報と自身が記憶している情報(2)を所定のアルゴリズムで

結合して情報(3)を形成する。

⑥ユーザ装置２０は、情報(3)と原情報を照合し、情報(3)が原情報と一致する場合に、本人であることを確認する。

なお、ユーザ装置２０は、情報(1)を受信できない場合、あるいは受信した情報が情報(1)でない場合には、所定の処理を実行する。例えば、情報(1)の送信要求信号を送信した後、所定時間内に情報を受信できない場合には、再度送信要求信号を送信する。そして、所定回数送信要求信号を送信しても情報(1)を受信できない場合には、本人を確認できないと判断し、所定の終了処理を実行する。例えば、エラーメッセージを認証端末装置に表示させる。

【００１１】次に、原情報を分割、結合する方法を具体的に説明する。第１の例を図４に示す。本実施例では、原情報［０１１１］を情報(1)［００１１］と情報(2)［０１０１］に分割している。そして、一方（例えば、情報(1)）をユーザ携帯装置１０に記憶させ、他方（例えば、情報(2)）と原情報をユーザ装置２０に記憶させる。ユーザ装置２０は、情報を受信すると、受信した情報と自身が記憶している情報(2)を所定のアルゴリズムで結合して情報(3)を形成する。本実施例では、受信した情報と情報(2)をＯＲ処理する。受信した情報が情報(1)の場合には、受信した情報と情報(2)をＯＲ処理することによって、原情報［０１１１］が形成される。さらに、情報(3)と原情報とを照合して本人確認を行う。本実施例では、情報(3)が原情報と同じである否かを判断する。例えば、情報(3)と原情報をＸＯＲ（排他的論理和）処理する。分割方法は、図４に示した例に限定されず、分割した情報(1)と情報(2)を所定の論理演算することによって原情報を形成することができればよい。

【００１２】第２の例を図５に示す。本実施例では、原情報［数字７の図形のビット行列］を、図５で左右に引いた分割線を境に、上部の情報(1)と下部の情報(2)に分割する。そして、一方（例えば、情報(1)）をユーザ携帯装置１０に記憶させ、他方（例えば、情報(2)）と原情報をユーザ装置２０に記憶させる。ユーザ装置２０は、情報を受信すると、受信した情報と自身が記憶している情報(2)を所定のアルゴリズムで結合して情報(3)を形成する。本実施例では、受信した情報のビット行列と情報(2)のビット行列を結合する。受信した情報が情報(1)の場合には、受信した情報のビット行列と情報(2)のビット行列を結合すると、原情報［数字７の図形のビット行列］が形成される。さらに、情報(3)と原情報を照合して本人確認を行う。本実施例では、情報(3)のビット行列で表される図形が、原情報のビット行列で表される図形と同じであるか否かを判断する。分割線を引く場所、引き方、分割線の本数等は、適宜選択可能である。

【００１３】なお、原情報を分割する数や分割する位置等は種々変更可能である。例えば、原情報を第１情報、第２情報、第３情報に分割し、第１情報と第３情報を情報(1)とし、第２情報を情報(2)としてもよい。また、情報(1)及び情報(2)として同じ情報を用いることもできる。この場合、例えば、情報(2)［０１１１］（＝情報(1)）と原情報［００００］をユーザ装置２０に記憶させる。ユーザ装置２０は、受信した情報と自身が記憶している情報(2)をＸＯＲ処理して情報(3)を形成する。そして、情報(3)と原情報を照合して本人確認を行う。受信した情報と自身が保有している情報を結合するアルゴリズムは、原情報をを分割する分割方法によって決定される。

【００１４】次に、本発明の本人確認装置の第１の実施の形態のブロック図を図６に示す。本実施の形態の本人確認装置は、ユーザ携帯装置１０ｂとユーザ装置２０ｂを有している。ユーザ携帯装置１０ｂは、信号出力手段１１ｂ、変調／復調手段１２ｂ、通信手段１３ｂにより構成されている。信号出力手段１１ｂは、例えば、一方の分割情報である情報(1)を記憶する記憶手段を有し、情報(1)を出力する。情報(1)の形式としては、種々の形式を用いることができる。変調／復調手段１２ｂは、信号出力手段１１ｂから出力された情報(1)を変調し、通信手段１３ｂを介して送信する。あるいは、変調／復調手段１２ｂは、通信手段１３ｂを介して受信した信号を復調する。そして、復調した信号に情報(1)の送信要求信号が含まれている場合には、情報(1)を変調し、通信手段１３ｂを介して送信する。ユーザ携帯装置１０ｂには、各手段に電力を供給する電池が設けられている。ユーザ装置２０ｂは、通信手段２１ｂ、変調／復調手段２２ｂ、結合手段２３ｂ、信号出力手段２４ｂを有している。変調／復調手段２２ｂは、通信手段２１ｂを介して受信した信号を復調し、結合手段２３ｂに出力する。あるいは、変調／復調手段２２ｂは、情報(1)の送信要求信号を変調し、通信手段２１ｂを介して送信する。そして、その後に通信手段２１ｂを介して受信した信号を復調し、結合手段２３ｂに出力する。信号出力手段２４ｂは、例えば、他方の分割情報である情報(2)を記憶する記憶手段を有し、情報(2)を出力する。結合手段２３ｂは、変調／復調手段２２ｂから入力された信号（情報(1)）と情報(2)を所定のアルゴリズムで結合して情報(3)を形成する。例えば、割り符を合わせる方法を用いて情報(1)と情報(2)を結合する。さらに、結合手段２３ｂ（本人確認手段）は、情報(3)と原情報の照合結果に基づいて本人か否かを確認する。結合手段２３ｂは、信号出力手段２４ｂあるいは変調／復調手段２２ｂと一体に設けてもよい。ユーザ装置２０ｂには、各手段に電力を供給する電池が設けられている。結合手段２３ｂは、例えば、出力禁止信号を出力する。結合手段２３ｂから出力禁止信号が出力されていると、ユーザ機器は使用不能となる。例えば、デビットカードに記憶されているカード情報を認証端末装置で読み取ることができない、あ

るいは携帯電話を使用することができない。なお、原情報は、ユーザ装置２０ｂの信号出力手段２４ｂに記憶させてもよい。

【００１５】ユーザ装置とユーザ機器が別体の場合には、ユーザ装置（結合手段）とユーザ機器との間の信号の伝送は、無線あるいはケーブルを介して行われる。なお、ユーザ装置及びユーザ機器に互いに接続可能な接続端子を設けておけば、接続端子同士を接続するだけでユーザ装置とユーザ機器を接続することができるため、接続作業が容易となる。なお、ユーザ携帯装置１０ｂの信号出力手段１１ｂ、変調／復調手段１２ｂ、通信手段１３ｂや、ユーザ装置２０ｂの通信手段２１ｂ、変調／復調手段２２ｂ、結合手段２３ｂ、信号出力手段２４ｂは、ハードウェアで実現してもよいし、ソフトウェアで実現してもよい。本実施の形態の結合手段２３ｂが、本発明の本人確認手段に対応する。

【００１６】図７は、ユーザ機器４０ｂの１実施例の斜視図である。図７に示すユーザ機器４０ｂは、カード状に形成されている。そして、カードの内部に、図６に示した各手段２１ｂ～２４ｂが設けられている。ユーザ機器４０ｂは、ユーザ携帯装置１０ｂと通信を行う通信機能を備えた通信機器でもある。ユーザ機器４０ｂとしては、磁気カード、ＩＣカード、デビットカード、クレディットカード、キャッシュカード等を用いることもできる。例えば、デビットカード、クレディットカードまたはキャッシュカード等の決済用カードに通信手段を設けることによって、決済用カードに本人確認機能を持たせることができる。なお、カードは、決済用カードや金融用カードに限定されるものではなく、無線機等の通信機器をカード状に形成したものでもよいことは、勿論である。

【００１７】図８は、本発明の本人確認方法の第２の実施の形態の概略図である。本実施の形態は、携帯電話機４０ｃをユーザ機器として用いている。本実施の形態では、携帯電話機４０ｃは、本人確認処理を行い、その結果に基づいて通信を許可するか否かを判断している。例えば、携帯電話機４０ｃに設けられているユーザ装置２０ｃは、ユーザ携帯装置１０ｃから送信される情報(1)が、自身が記憶している情報(2)に対応する正しい情報である場合にのみ、携帯電話機４０ｃの使用を許可する。これにより、携帯電話機４０ｃの不正使用を防止することができる。なお、ユーザ機器４０ｃとしては、携帯電話機の他に、通信機能を備える各種の機器を用いることができる。例えば、ＰＨＳ（Personal Handyphone System）電話機、ＰＤＡ（Personal Data Assistance、個人用携帯情報端末）無線機、ＥＴＣ（Electronic Toll Collection System, ノンストップ自動料金支払システム）用通信機、ＩＴＳ（Intelligent Transport Systems, 高度道路交通システム）用の車両通信機、電話通信端末（例、公衆電話機、ＦＡＸ端末）、データ通信端末（例、パソコン）等を用いることができる。何をユーザ機器として用いるかは、営業上または設計上の選択事項である。また、携帯電話機４０ｃと端末装置２ｃとの接続は、通信回路網４ｃを介して行ってもよい。携帯電話機４０ｃと端末装置（例えば、認証端末装置）２ｃとの間の接続方法や通信方法は種々の方法を用いることができる。

【００１８】図９は、本発明の本人確認方法の第３の実施の形態の概略図である。本実施の形態では、ユーザ携帯装置１０ｄをＩＣチップで構成し、ユーザ携帯機器（指輪）３０ｄに取り付けている。勿論、ユーザ携帯機器３０ｄを指輪以外のもの（例えば、ベルトのバックル、ブレスレット、ペンダント、イアリング、ピアス等）に取り付けてもよい。本実施の形態では、ユーザ装置２０ｄもＩＣチップで構成し、無線機４０ｄに取り付けている。ＩＣチップは、集積回路（ＩＣ）をパッケージあるいはモールドし、リード線（外部端子）を備えるＩＣ製品である。ＩＣには、ＬＳＩ（Large Scale Integration）やＶＬＳＩ等も当然に含まれる。回路の集積度は問題ではない。なお、ユーザ携帯装置及びユーザ装置のいずれかをＩＣチップとしてもよいし、両方をＩＣチップとしてもよいことは言うまでもない。さらに、ユーザ装置及びユーザ装置の一部をＩＣチップとしてもよい。

【００１９】図１０は、本発明の本人確認方法の第４の実施の形態の概略図である。本実施の形態では、ユーザ携帯装置１０ｅをユーザ携帯機器（眼鏡）３０ｅに取り付けている。例えば、接着剤により取り付けている。また、携帯電話機４０ｅをユーザ機器として用いている。ユーザ携帯装置１０ｅと携帯電話機２０ｅに設けられているユーザ装置２０ｃとの間の通信は、無線で行っている。ユーザ携帯装置１０ｅは、ＩＣチップでもよい。携帯電話機４０ｅに代えて、ＩＣカードやＩＣカード製のデビットカード等を用いてもよい。あるいは、携帯電話機能付きのＩＣカード等を用いることもできる。また、ユーザ携帯装置１０ｅは、眼鏡以外のもの、例えば、ブレスレットやベルト等に取り付けてもよい。あるいは、ユーザ携帯装置１０ｅを、ユーザ１のポケットやカバンに入れて持ち歩いてもよい。

【００２０】図１１は、本発明の本人確認装置の第２の実施の形態のブロック図である。本実施の形態では、ユーザ携帯装置１０ｆやユーザ装置２０ｆの構成要素の一部あるいは全部を、ＩＣチップで構成している。図１１では、ユーザ携帯装置１０ｆの信号出力手段１１ｆ、変調／復調手段１２ｆ及び通信手段１３ｆのそれぞれをＩＣチップで構成している。もちろん、これら３つの手段を一つのＩＣチップで構成することもできる。また、ユーザ装置２０ｆの信号出力手段２４ｆをＩＣチップで構成している。なお、ユーザ装置２０ｆの通信手段２１ｆ、変調／復調手段２２ｆ、結合手段２３ｆ及び信号出

力手段２４ｆを一つのＩＣチップ２５ｆで構成することもできる。

【００２１】図１２は、本発明の本人確認装置の第３の実施の形態のブロック図である。本実施の形態では、ユーザ装置２０ｇ（例えば、信号出力手段２４ｇ）に、破壊手段２６ｇを設けている。破壊手段２６ｇは、所定の情報（例えば、信号出力手段２４ｇに記憶されている情報(2)）の不正な読み出しを検出した場合に、信号出力手段２４ｇから所定の情報が外部に出力されるのを阻止する。不正な読み出しの検出は、例えば、通信手段２１ｇで受信した信号に、正規の読み出し信号以外の読み出し信号が含まれていることにより検出する。信号出力手段２４ｇからの信号出力を阻止する方法としては、例えば、信号出力手段２４ｇに過電流を流し、信号出力手段２４ｇを破壊する方法を用いることができる。あるいは、揮発性の記憶手段に情報等を記憶させている場合には、記憶手段への電源供給を遮断し、記憶手段に記憶されている情報等を消去する方法を用いてもよい。なお、破壊手段２６ｇは、ユーザ装置２０ｇが分解されることを検出した場合に、信号出力手段２４ｇあるいはユーザ装置２０ｇを破壊するものでもよい。本実施の形態の破壊手段２６ｇが、本発明の読出禁止手段に対応する。

【００２２】図１３は、本発明の本人確認装置の第４の実施の形態のブロック図である。本実施の形態では、ユーザ携帯装置１０ｈの変調／復調手段１４ｈに、暗号化機能を持たせている（暗号化機能及び暗号解読機能を持たせる場合もある）。また、ユーザ装置２０ｈの変調／復調手段２７ｈに、暗号解読機能を持たせている（暗号化機能及暗号解読機能を持たせる場合もある）。本実施の形態では、例えば、ユーザ携帯装置１０ｈから情報(1)をユーザ装置２０ｈに送信する場合に、情報(1)を暗号化して送信することができる、これにより、セキュリティが一層向上する。なお、ユーザ装置２０ｈからユーザ携帯装置１０ｈに信号を送信する時にも、信号を暗号化してもよい。なお、暗号化機能と暗号解読機能を同じ手段で行ってもよいし、異なる手段で行ってもよい。暗号化方法としては、公知の種々の方法を用いることができる。

【００２３】図１４は、本発明の本人確認装置の第５の実施の形態のブロック図である。本実施の形態では、ユーザ携帯装置１０ｉの変調／復調手段１１ｉに、送信信号にランダムノイズ（ＲＮ）を挿入する機能を持たせている（ＲＮ挿入機能及びＲＮ解除機能を持たせる場合もある）。また、ユーザ装置２０ｉの変調／復調手段２８ｉに、受信した信号からランダムノイズ（ＲＮ）を除去する機能を持たせている（ＲＮ挿入機能及びＲＮ除去機能持たせる場合もある）。本実施例では、例えば、ユーザ携帯装置１０ｉから情報(1)をユーザ機器２０ｉに送信する場合に、情報(1)にランダムノイズを挿入して送信することができる。これにより、セキュリティが一層向上する。なお、ランダムノイズの挿入機能とランダムノイズの除去機能を同じ手段で行ってもよいし、異なる手段で行ってもよい。また、信号の漏洩を防止する手段としては，ランダムノイズを挿入する方法以外にも公知の種々の方法を用いることができる。

【００２４】図１５は、本発明の本人確認装置の第６の実施の形態のブロック図である。本発明の本人確認装置を用いても、本人確認情報である情報(1)や情報(2)が第三者に漏れる可能性はある。情報(1)あるいは情報(2)が漏れている可能性がある場合には、情報(1)及び情報(2)を取り替えればよい。そこで、本実施の形態では、ユーザ携帯装置１０ｊの信号出力手段１１ｉ、ユーザ装置２０ｊの信号出力手段２４ｊを交換可能に構成している。図１５では、ユーザ携帯装置１０ｊの信号出力手段１１ｊ、変調／復調手段１２ｊ及び通信手段１３ｊを一つのＩＣチップ１６ｊで構成し、ユーザ装置２０ｊの通信手段２１ｊ、変調／復調手段２２ｊ、結合手段２３ｊ、信号出力手段２４ｊ及び破壊手段２６ｊを一つのＩＣチップ２５ｊで構成している。そして、ユーザ携帯装置１０ｊのＩＣチップ１６ｊを交換用のＩＣチップ１７ｊに、また、ユーザ装置２０ｊのＩＣチップ２５ｊを交換用のＩＣチップ２７ｊに交換可能に構成されている。なお、ＩＣチップの構成は種々変更可能である。例えば、ユーザ携帯装置１０ｊの信号出力手段１１ｊ、ユーザ装置２０ｊの信号出力手段２４ｊのみを交換可能に構成することもできる。また、ＩＣチップを交換可能に構成する方法としては、例えば、ピンやソケットにＩＣチップを差し込めるような構造にする方法等がある。

【００２５】以上の説明では、ユーザ携帯装置とユーザ装置との間の情報の送受信を非接触で行ったが、接触させた状態で情報の送受信をおこなうこともできる。例えば、ユーザ携帯機器としての磁気的あるいは電気的なＩＤカード、ＩＤカードタグ、携帯電話機を、ユーザ機器としてのパソコンのカード挿入口に差込みあるいはケーブルで接続しても良い。この場合、ＩＤカードあるいは携帯電話機から第１情報をパソコンに送信する。パソコンは、受信した情報と自己が保有する情報とを結合して原情報を形成することができた場合には、パソコンの使用を許可する。あるいは、逆に、パソコンをユーザ携帯装置、ＩＤカードや携帯電話機をユーザ機器として用いることもできる。

【００２６】

【発明の効果】本発明は、以下に記載する効果を有する。本発明は、生体情報、暗証番号、サイン（署名）、印章あるいはＩＤコード等を用いるのでなく、割り符のような、元々は一つの情報または信号を分割した情報を用いている。そして、各分割情報を、ユーザが携帯するユーザ携帯装置とユーザが使用するユーザ機器に設けられるユーザ装置にそれぞれ保持させ、ユーザ携帯装置とユーザ装置が保持している情報を結合（割り符合わせ）

を行って本人確認を行っている。このような情報は、生体情報のように変動することがない。また、通信手段や各情報の結合手段等は、ＩＣチップ等によって簡単に、安価に構成することができる。したがって、精度が高く、かつ低コストで本人確認を行うことができる。また、本発明では、ユーザ携帯装置が保有している情報とユーザ機器で保有している情報が結合されて元の情報（原情報）が復元されない限り、本人確認が行われない。このため、暗証番号やカードやＩＤタグ等を盗まれても不正使用の心配がない。つまり、ユーザ装置及びユーザ携帯装置を落としたり、盗まれたりしない限り、不正使用の恐れはない。ユーザ携帯装置をＩＣチップで構成すれば、ユーザが携帯可能な多くの部材（例えば、指輪やメガネ）に取り付けることができる。この場合、ユーザ携帯機器を、ユーザが自分で決めた部材に取り付けることができるので、ユーザ携帯機器が盗まれる恐れもほとんどない。万一、情報が漏れている恐れがある場合には、ユーザ携帯機器及びユーザ機器の所定のＩＣチップを新たなチップに交換すればよい。以上のように、本発明を用いることにより、不特定多数のユーザに対して、簡単、低コスト、高信頼性、高セキュリティで本人確認処理を行うことができる。本発明は、前記した実施例の構成に限定されることなく、本発明の要旨を変更しない範囲で種々の変更、追加、削除が可能である。例えば、ユーザ装置とユーザ機器との組付け形態、ユーザ携帯装置とユーザ携帯機器との組付け形態は、一体構成あるいは別体構成等種々変更可能である。例えば、ユーザ携帯装置をＩＣチップで形成するとともに、ＩＣチップをユーザ携帯機器（腕時計、眼鏡等）に接着剤や接着テープ等によって貼り付けることもできる。また、ユーザ装置とユーザ機器を一体に構成することもできる。また、ユーザ装置を構成する手段をユーザ機器を構成する手段と兼用してもよい。なお、ユーザ携帯装置がユーザ携帯機器に一体的に設けられている場合、ユーザ装置がユーザ機器に一体的に設けられている場合には、ユーザ携帯装置及びユーザ装置は、それぞれユーザ携帯機器及びユーザ機器ということもできる。また、１台のユーザ携帯装置と１台のユーザ装置により本人確認装置を構成したが、複数台のユーザ携帯装置により本人確認装置を構成することもできる。この場合には、例えば、原情報を分割してＮ個の分割情報を形成し、第１分割情報～第（Ｎ－１）分割情報をそれぞれ第１ユーザ携帯装置～第（Ｎ－１）ユーザ携帯装置に記憶させるとともに、第Ｎ分割情報をユーザ装置に記憶させる。そして、ユーザ装置（本人確認手段）は、受信した情報を所定のアルゴリズムで結合して原情報を形成することができた場合にユーザがそのユーザ機器の本来のユーザであることを確認する。

【００２７】以上説明したように、請求項１～５に記載の本人確認方法及び請求項６～請求項１３に記載の本人確認装置を用いれば、安価に、高い信頼性で本人を確認することができる。

【図面の簡単な説明】

【図１】本発明の本人確認方法の第１の実施の形態の概略図である。

【図２】本発明の本人確認方法の処理手順の１例を説明する図である。

【図３】本発明の本人確認方法の処理手順の他の例を説明する図である。

【図４】原情報を分割する１例を説明する図である。

【図５】原情報を分割する他の例を説明する図である。

【図６】本発明の本人確認装置の第１の実施の形態のブロック図である。

【図７】ユーザ機器の１実施例を示す図である。

【図８】本発明の本人確認方法の第２の実施の形態の概略図である。

【図９】本発明の本人確認方法の第３の実施の形態の概略図である。

【図１０】本発明の本人確認方法の第４の実施の形態の概略図である。

【図１１】本発明の本人確認装置の第２の実施の形態のブロック図である。

【図１２】本発明の本人確認装置の第３の実施の形態のブロック図である。

【図１３】本発明の本人確認装置の第４の実施の形態のブロック図である。

【図１４】本発明の本人確認装置の第５の実施の形態のブロック図である。

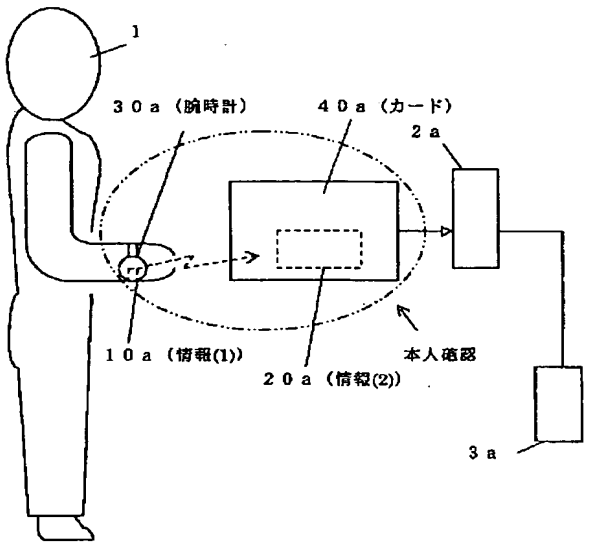
【図１５】本発明の本人確認装置の第６の実施の形態のブロック図である。

【符号の説明】

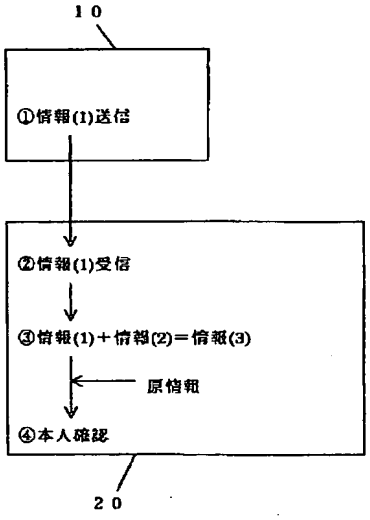
１　ユーザ
２ａ　認証端末装置
３ａ　認証センタ
１０、１０ａ～１０ｊ　ユーザ携帯装置
２０、２０ａ～２０ｊ　ユーザ装置
３０ａ、３０ｄ、３０ｅ　ユーザ携帯機器
４０ａ～４０ｅ　ユーザ機器
１１ｂ、１１ｆ、１１ｇ～１１ｊ　信号出力手段
１２ｂ、１２ｆ、１２ｇ、１２ｊ　変調／復調手段
１３ｂ、１３ｆ、１３ｇ～１３ｊ　通信手段
１４ｈ、２７ｈ　変調／復調手段（暗号機能）
１５ｉ、２８ｉ　変調／復調手段（ＲＮ機能）
１６ｊ、１７ｊ、２５ｆ、２５ｇ、２５ｊ、２７ｊ　ＩＣチップ
２１ｂ、２１ｆ～ｊ　通信手段
２２ｂ、２２ｆ、２２ｇ、２２ｊ　変調／復調手段
２３ｂ、２３ｆ～ｊ　結合手段（本人確認手段）
２４ｂ、２４ｆ、２４ｇ、２４ｈ、２４ｊ　信号出力手段

２６ｇ、２６ｊ　破壊手段（読出禁止手段）

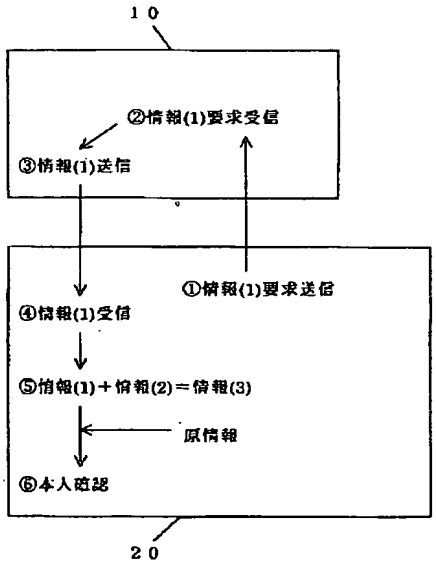
【図１】



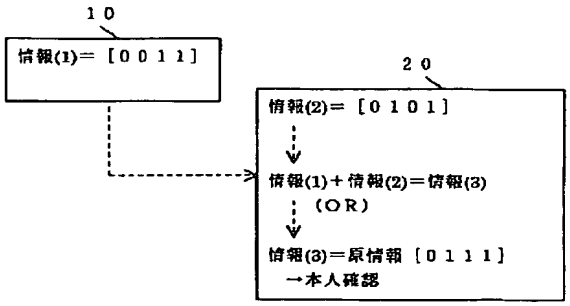
【図２】



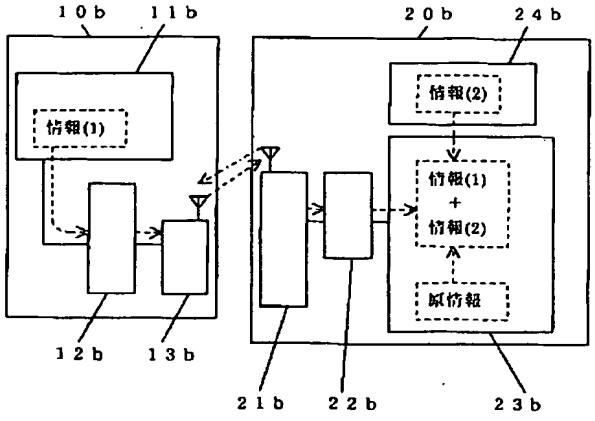
【図３】



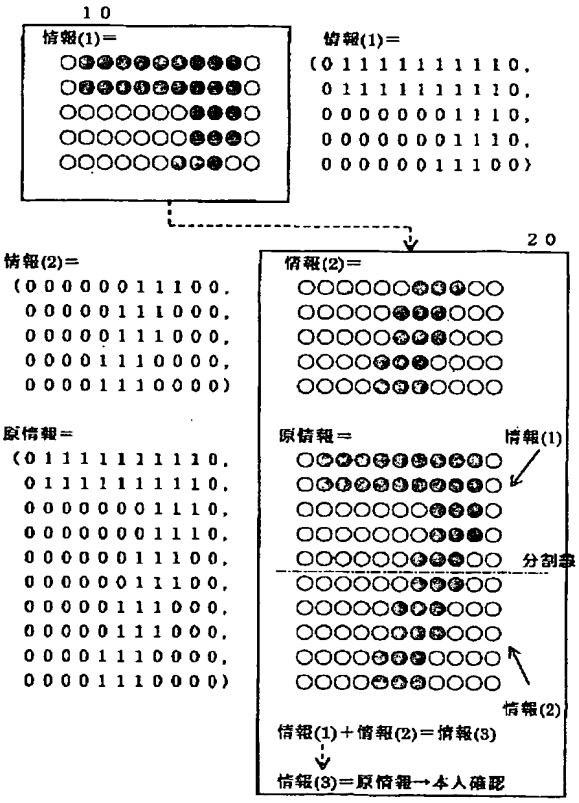
【図４】



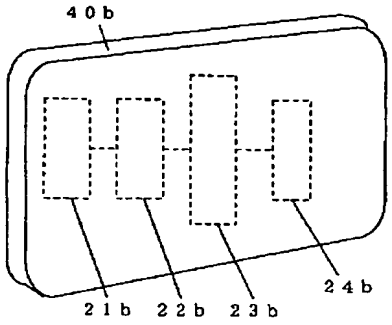
【図６】



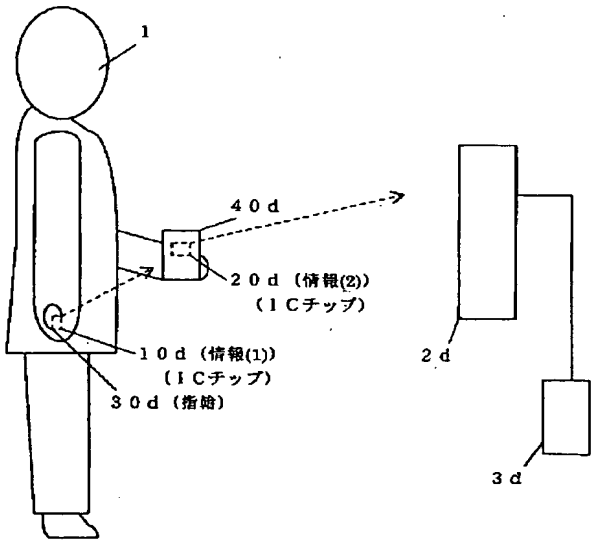
【図５】



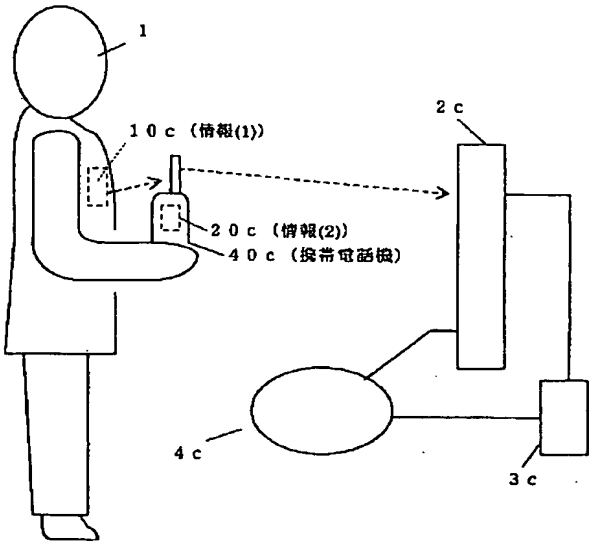
【図７】



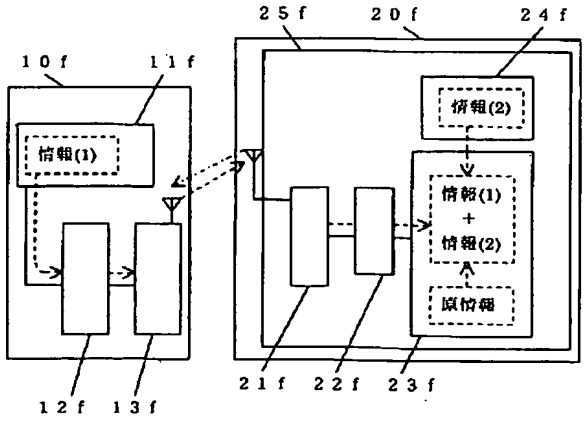
【図９】



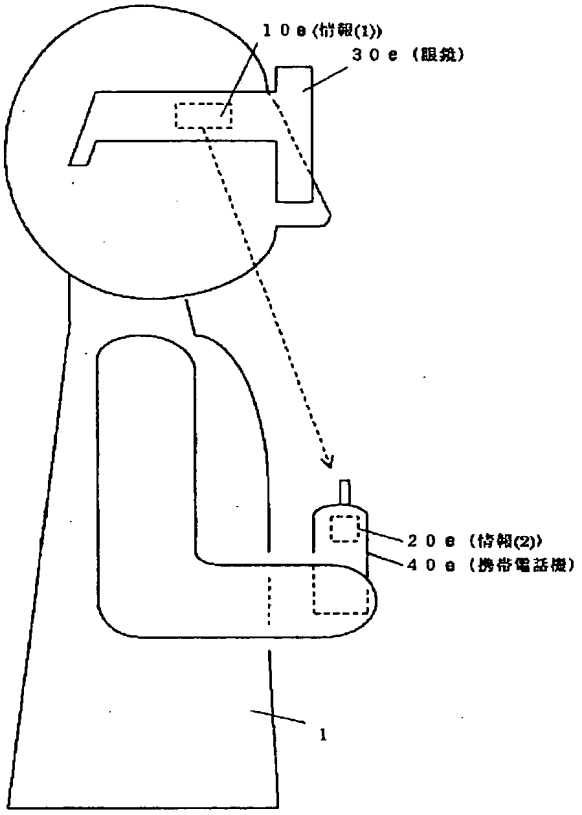
【図８】



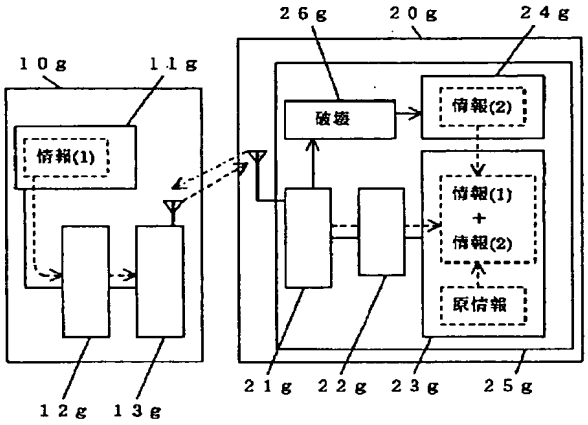
【図１１】



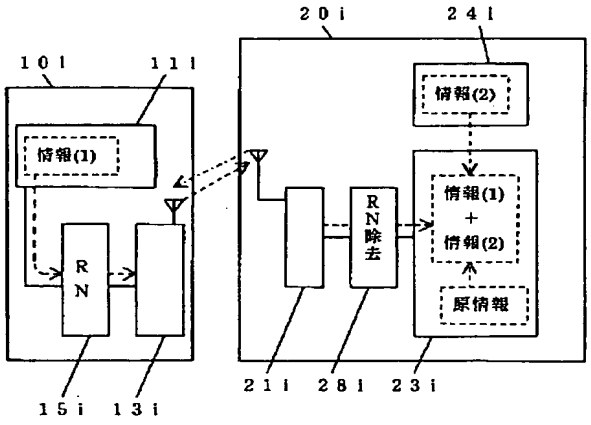
【図１０】



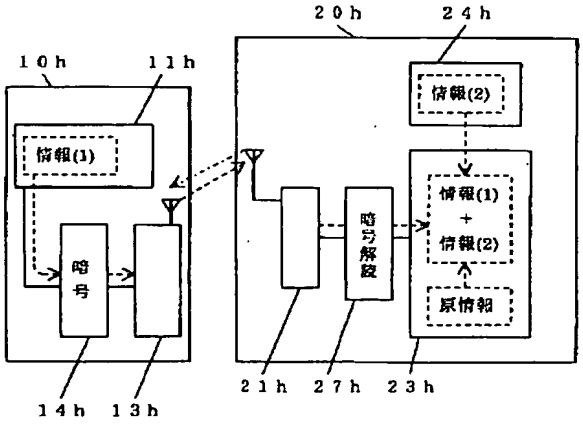
【図１２】



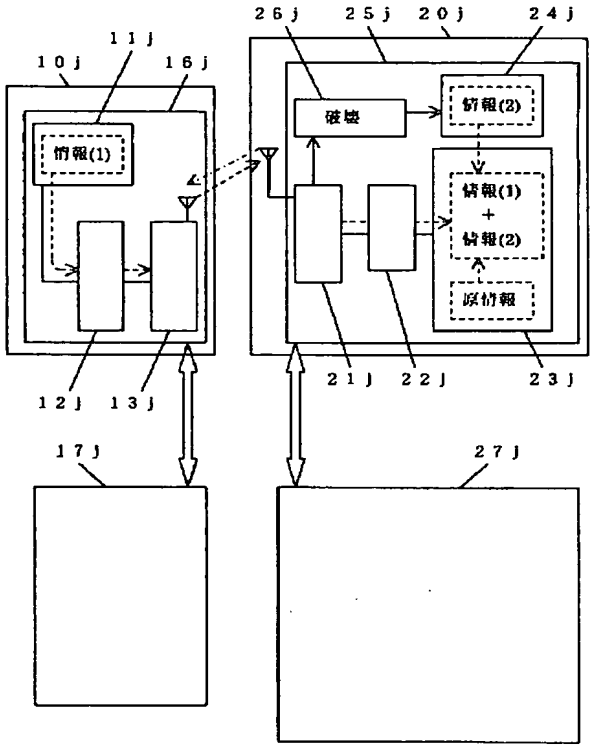
【図１４】



【図１３】



【図１５】



フロントページの続き

(72)発明者　深津　博一
名古屋市南区千竈通２丁目13番地１　株式
会社タイテック内

Ｆターム(参考)　5B085 AE02 AE23